DELL Technologies

Solution Brief

Safeguard Your Infrastructure from Ransomware and Cyber Threats

Dell EMC Storage portfolio delivers secure, robust, and scalable storage solutions for all your critical workload needs

---

This brief highlights Dell Technologies' methodologies, processes, and tools to implement cutting-edge security practices while governing compliance and industry standards.

Data value brings opportunity and risk

Data, the new currency of the global economy, has become the single most valuable asset for a majority of businesses[1] The evolving ability to mine data for profitable insights is driving organizations to create and capture more of it – harvesting and manipulating it in more locations and under more circumstances. This has driven a significant increase in overall data volumes, but also an explosion in data diversity and distribution. In just a few short years, it's become axiomatic that data is gathered, stored and processed everywhere, from edge to core to cloud. The opportunities to capitalize on this data and drive business value appear to be endless.

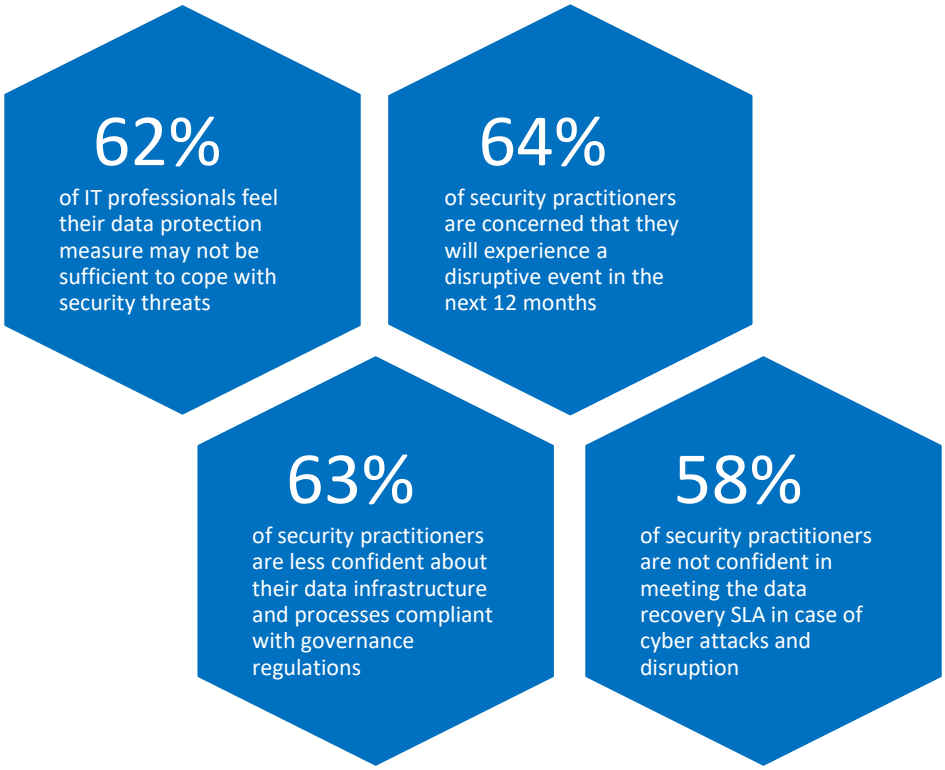
Unfortunately, this newly distributed value also represents a target. Dynamically connected e-commerce built on a rapidly-shifting mix of technologies, an exponential increase in remote work, and the general "hyper-connectivity" of our digital lives now provide the largest IT attack surface in history, as malicious actors regularly disrupt businesses for financial gain and other harmful purposes.

Whether their ultimate motivation is ideological, political, or economic, today's cybercriminals simultaneously exploit security vulnerabilities at a physical, logical, and component level, probing hardware, software, and "human" aspects of any system. Experienced and would-be attackers have available a virtual marketplace of tools and techniques, ranging from rudimentary to sophisticated approaches, including spam, malware, ransomware, and zero-day attack. Bad actors of every kind have ample opportunity to misuse, destroy or hold hostage your critical data – and according to the Cybersecurity Ventures report, a successful cyber or ransomware attack occurs **every 11 seconds**, at a staggering estimated global cost of **$6 trillion** in 2021.

Aware, but not prepared

The threat is well-known, as is the importance of maintaining data confidentiality, availability, and integrity. Cyber-resilience strategies of one form or another have become mandates for virtually all organizations and government leaders, and are even seen as a competitive advantage in today's data-driven world.

However, despite this knowledge and prioritization, few organizations are actually confident in their ability to protect against and recover from a sophisticated cyberattack (GDPI 2021). Dell's Global Data Protection Index 2021 report reveals that the majority of IT professionals are aware of and concerned about the impact an attack could have on their organization – yet at the same time, 62%[1] feel their data protection measures may not be sufficient to cope with even current malware, ransomware, and other threats. More alarming, when looking forward, 82% have concerns their existing solutions won't address future security challenges.



Why is this the case? We believe it reflects the difficult balancing act businesses must undertake to execute effective security risk management while also achieving their business goals of time-to-market, flexibility, simplicity, and overall cost control. In most companies, human organizations and vital technology infrastructure have each grown up without addressing modern security needs – and for many companies, layering on adequate security as an afterthought or standalone project is prohibitively disruptive and painfully expensive, despite the very real cost of "doing nothing."

Need a holistic, business-centric approach

Today's organizations need more than a point add-on solution to security. A successful plan must take into account an entire ecosystem of end-to-end technology and environmental factors, as well as the specific strategic and financial directives that make each industry and company unique.

As a global leader in cloud, IT, and mobile infrastructure, Dell is uniquely positioned to help companies move forward. Our trusted infrastructure, virtual compute, network, and storage technologies support the majority of the world's workloads in thousands of data centers around the world. We've seen more than our share of cyberattacks at every level – but just as importantly, we understand the business risks and challenges of addressing them.

Dell Technologies Security Methodology

Dell's approach is holistic and business-centric, with comprehensive methods that integrate end-to-end security throughout the product and solution life cycle. Dell's security methodologies apply to every product in our portfolio, beginning during the requirements phase and continuing through the design, release, and after-sales support phases.

Security in our DNA

At Dell, security and resiliency are everyone's responsibility, and before our developers even begin work on products, we provide rigorous training on job-specific best practices and policies to create a security-aware culture across our entire development community.

Dell practices an embedded intrinsic security posture from code to deployment

One aspect of that training is Dell's Secure Development Lifecycle (SDL), which defines the security controls that product teams adopt while developing new features and functionality. Dell hardware and software engineers are required to follow a set of strict procedures to prevent weaknesses and vulnerabilities from being introduced – either by our own development or by third-party components.

Dell's SDL includes analysis and prescriptive controls around key risk areas, encompassing threat modeling, static code study, component management, and regular testing. We leverage a variety of industry and in-house tools including CVE (Common Vulnerabilities and Exposures) and CWE (Common Weaknesses Enumeration) published by MITRE, the OWASP (Open Web Application Security Project) Top 10, and the SANS Top 25 Most Dangerous Software Errors. Dell also collaborates through many industry-standard venues such as Software Assurance Forum for Excellence in Code (SAFECode), Building Security In Maturity Model (BSIMM), and IEEE Center for Secure Design to ensure that industry practices are followed.

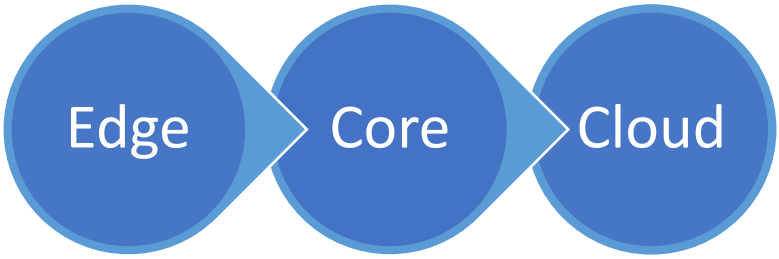
Ongoing security support

Once our customers receive their Dell product, our security development program does not end – its focus shifts to the new vulnerabilities (particularly software- and firmware-related) that are discovered regularly across the industry. Dell's Product Security Incident Response Team (PSIRT) oversees the Vulnerability Response Program (VRP) and is responsible for coordinating the response and disclosure for all identified product vulnerabilities. Dell's Vulnerability Response Policy aligns to industry best practices from the Forum for Incident Response and Security Teams (FIRST) PSIRT Framework, ISO/IEC 29147, and ISO/IEC 30111. Dell provides customers with timely information, guidance, and mitigation options to minimize risks associated with security vulnerabilities and discloses all vulnerabilities on Dell's Security Advisories and Notices portal.

Dell's SDL and VR programs are integrated into Dell's overall product lifecycle governance processes, which include a business readiness review as well as an internal security assessment of each product.

Development outcomes

Dell's relentless cybersecurity focus during development, combined with our broad business use case experience, culminates in a world-class portfolio of secure systems, solutions, and services. Whether those systems run at the edge, in a core data center or co-location facility, or in a cloud, they provide the trusted infrastructure foundation that enables next-gen innovation.

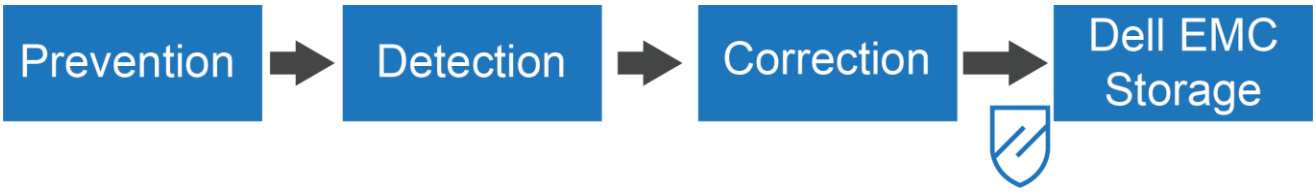


Dell EMC Power Portfolio

PowerEdge; PowerMax; PowerStore; PowerScale; PowerFlex; PowerVault; PowerProtect

Because solution targets vary across our diverse portfolio, different security capabilities are deployed depending on the business requirements driving each product. From Hardware Root of Trust in the PowerEdge line of servers to end-to-end encryption in PowerMax, we seek to meet unique business security needs in the most cost-effective, automated, and future-proof manner possible.

Each Dell Technologies product solution offers a range of security capabilities within the following general categories.



Prevention

The first element of resilient cybersecurity is prevention. Preventing malicious activities, unauthorized user access, and hardening all access points to storage reduces risk. Dell Technologies storage products offer robust role-based access control (RBAC) to allow only authorized users to perform designated operations like provisioning storage, network administration, and establishing VMware settings. Furthermore, PowerMax offers a Secure snap option to cement data security by preventing snapshots deletion from malicious actors.

Dell storage solutions incorporate advanced multi-factor authentication to control sensitive storage operations, firewall/Secure Host ID/SAN port locking to allow only authorized hosts access. Tamper-proof audit logs track system usage and changes, so IT admins can identify and act on suspicious activity.

Dell also makes sure your data-at-rest stays safe. Data encryption protects flash drive media from unauthorized access even if it's removed from the data center—while adhering to stringent FIPS 140-2 security requirements and controlled key management functions to achieve the highest security trust as a data custodian without compromising performance and scalability.

Detection

After taking all steps toward prevention, Dell storage constantly monitors system activities for suspicious events using machine learning-enabled tools and processes to thwart any harmful impacts quickly. Dell's storage products seamlessly integrate with CloudIQ, Dell's AIOps application for infrastructure performance, capacity, and security monitoring, analytics, and recommendations. CloudIQ Cybersecurity notifies you of infrastructure security misconfigurations by comparing actual to desired configurations (e.g., based on NIST 800-53 r5 and NIST 800 – 209 standards) and recommends actions for remediation. These intelligent insights help you maintain the security health status of your storage environment.

Ransomware Defender for PowerScale puts IT teams a step ahead of cyber attackers by detecting unusual data access patterns and suspicious behavior that are indicative of a ransomware attack.

Correction

Correcting issues quickly and restoring an operational state of the infrastructure yields a huge positive business outcome. Dell EMC storage products offer robust data availability and recoverability using proven services such as local and remote data replications, direct data backup and recovery capabilities, and cyber recovery with air gap protection to protect against ransomware and other modern threats.

Dell's storage products are backed by the most stringent corporate compliance and security regulatory requirements including FIPS 140-2 validation, Common Criteria, STIG hardening (Security Technical Implementation Guides), and the U.S. Department of Defense Approved Products List certification to name a few.

Conclusion

Cyber attacks will continue to be a threat to businesses, but with Dell Technologies you can have peace of mind that your data and IT assets are secure, protected, and available. We stop at nothing to help thwart threats with intrinsically secure infrastructure and devices, comprehensive detection and response, data protection, and cyber-recovery.

Over 95% of Fortune 100 companies use Dell's reliable storage products to run their critical workloads in delivering business values. The top financial, healthcare, transportation, telecommunications, retailing, energy, aerospace & defense companies use Dell's differentiated storage solutions to stay ahead of the IT transformation journey to deliver secure and optimized services to their users.

Next steps

Ready to enhance your data protection and improve the resiliency of your critical IT infrastructure? Dell's Cyber Resiliency Assessment is a free 5-minute security health check with expert insights and recommendations from Enterprise Solution Group (ESG). Then check out Dell's 2021 Global Data Protection Index and visit the Dell Technologies Security webpage to learn more about how data protection plays a key role in transforming your IT and maximizing the value of your data. Additionally, watch a short PowerMax and PowerSore Cyber Resiliency video to gain security insight these products offer.

[1] "Based on research by Vanson Bourne commissioned by Dell Technologies, "Global Data Protection Index 2021 Snapshot," carried out February – March 2021. Results were derived from a total of 1,000 IT decision-makers worldwide from both private and public organizations with 250+ employees."